CLAIMS:

1. In an online commerce transaction system including a buyer, a seller, and an authentication service, a processor-implemented method for authenticating to the seller that the buyer is authorized to use a payment instrument as part of an online commerce transaction, the method comprising:

in real-time as part of the online commerce transaction, the authentication service performing the steps of:

receiving a request to verify that the buyer is authorized to use the payment instrument;

determining whether the buyer has access to secret information without revealing the secret information to the seller, wherein access to the secret information verifies authority to use the payment instrument; and

responsive to the determination of whether the buyer has access to the secret information, transmitting to the seller a response including whether the buyer is authorized to use the payment instrument.

2. The method of claim 1 wherein, in real-time as part of the online commerce transaction, the authentication service further performs the step of:

applying profile information about the buyer to the online commerce transaction.

3. The method of claim 1 further comprising:

responsive to a determination that the buyer has access to the secret information, the authentication service at least partially processing the payment instrument.

4. The method of claim 1 further comprising:

the authentication service storing a record of the use of the payment instrument.

5. The method of claim 4 wherein the record has been digitally signed by the buyer.

6. The method of claim 4 wherein the record has been digitally signed by the authentication service.

7. The method of claim 1 further comprising:

prior to the online commerce transaction, the authentication service performing the steps of:

receiving confirmation information which enables the authentication service to determine whether the buyer has access to the secret information; and

storing the confirmation information;

wherein the step of determining whether the buyer has access to secret information comprises:

retrieving the confirmation information; and

using the confirmation information to determine whether the buyer has access to the secret information.

8. The method of claim 1 wherein the step of receiving a request to verify that the buyer is authorized to use the payment instrument includes receiving the request as a result of an offer from the buyer to use the payment instrument.

9. The method of claim 1 wherein the online commerce transaction system is an HTTP-based web system.

10. The method of claim 9 wherein the secret information comprises a private key, and the private key and a corresponding public key form a key pair for use in public-key cryptography.

11. The method of claim 10 wherein in real-time as part of the online commerce transaction, the authentication service further performs the step of:

receiving an offer from the buyer to use the payment instrument, wherein the offer is digitally signed using the private key.

12. The method of claim 9 wherein the step of receiving a request to verify that the buyer is authorized to use the payment instrument comprises:

receiving the request as a result of the buyer submitting a form for the online commerce transaction using a web browser, the form comprising:

an action attribute identifying the authentication service; and

a method attribute for transmitting the request to the authentication service as a result of the buyer's submission of the form.

13. The method of claim 12 wherein:

the request further comprises an address for the seller; and

the step of transmitting to the seller a response comprises transmitting the response to the address included in the request.

14. The method of claim 9 wherein the step of determining whether the buyer has access to secret information comprises:

transmitting to the buyer a challenge request requesting proof that the buyer has access to the secret information;

receiving from the buyer a challenge response allegedly proving that the buyer has access to the secret information; and

determining on the basis of the challenge response whether the buyer has access to the secret information.

15. The method of claim 14 wherein the challenge request further comprises:

a description of the online commerce transaction for which the payment instrument is to be used; and

a request for the buyer's consent to use the payment instrument for the online commerce transaction.

16. The method of claim 9 wherein the step of transmitting to the seller a response including whether the buyer is authorized to use the payment instrument comprises POSTing the response to the seller.

17. A software program product for authenticating to a seller that a buyer is authorized to use a payment instrument as part of an online commerce transaction, the software program product controlling the operation of a processor by execution of the software by the processor, the software executing the steps of:

in real-time as part of the online commerce transaction:

receiving a request to verify that the buyer is authorized to use the payment instrument;

determining whether the buyer has access to secret information without revealing the secret information to the seller, wherein access to the secret information verifies authority to use the payment instrument; and

responsive to the determination of whether the buyer has access to the secret information, transmitting to the seller a response including whether the buyer is authorized to use the payment instrument.

18. The software program product of claim 17 wherein, in real-time as part of the online commerce transaction, the software further performs the step of:

applying profile information about the buyer to the online commerce transaction.

19. The software program product of claim 17 wherein the software further performs the step of:

responsive to a determination that the buyer has access to the secret information, at least partially processing the payment instrument.

20. The software program product of claim 17 wherein the software further performs the step of:

storing a record of the use of the payment instrument.

21. The software program product of claim 20 wherein the software further performs the step of:

digitally signing the record.

22. The software program product of claim 17 wherein the step of determining whether the buyer has access to secret information comprises:

retrieving confirmation information; and

using the confirmation information to determine whether the buyer has access to the secret information.

23. The software program product of claim 17 wherein the software program product is adapted for execution by a web server.

24. The software program product of claim 23 wherein the secret information comprises a private key, and the private key and a corresponding public key form a key pair for use in public-key cryptography.

25. The software program product of claim 24 wherein in real-time as part of the online commerce transaction, the software further performs the step of:

receiving an offer from the buyer to use the payment instrument, wherein the offer is digitally signed using the private key.

26. The software program product of claim 23 wherein the step of receiving a request to verify that the buyer is authorized to use the payment instrument comprises:

receiving the request as a result of the buyer submitting a form for the online commerce transaction using a web browser, the form comprising:

an action attribute identifying the authentication service; and

a method attribute for transmitting the request to the authentication service as a result of the buyer's submission of the form.

27. The software program product of claim 26 wherein:

the request further comprises an address for the seller; and

the step of transmitting to the seller a response comprises transmitting the response to the address included in the request.

28. The software program product of claim 23 wherein the step of determining whether the buyer has access to secret information comprises:

transmitting to the buyer a challenge request requesting proof that the buyer has access to the secret information;

receiving from the buyer a challenge response allegedly proving that the buyer has access to the secret information; and

determining on the basis of the challenge response whether the buyer has access to the secret information.

29. The software program product of claim 28 wherein the challenge request further comprises:

a description of the online commerce transaction for which the payment instrument is to be used; and

a request for the buyer's consent to use the payment instrument for the online commerce transaction.

30. The software program product of claim 23 wherein the step of transmitting to the seller a response including whether the buyer is authorized to use the payment instrument comprises POSTing the response to the seller.

31. An online commerce transaction system with buyer authentication comprising:

a seller;

a buyer desiring to use a payment instrument as part of an online commerce transaction with the seller; and

an authentication service communicatively coupled to the seller, for performing, in real-time as part of the online commerce transaction, the steps of:

receiving a request to verify that the buyer is authorized to use the payment instrument;

determining whether the buyer has access to secret information without revealing the secret information to the seller, wherein access to the secret information verifies authority to use the payment instrument; and

responsive to the determination of whether the buyer has access to the secret information, transmitting to the seller a response including whether the buyer is authorized to use the payment instrument.

32. The system of claim 31 wherein the authentication service is further adapted for storing a record of use of the payment instrument.

33. The system of claim 31 wherein the authentication service is communicatively coupled to the seller using the HTTP protocol.

34. The system of claim 31 wherein the secret information comprises a private key, and the private key and a corresponding public key form a key pair for use in public-key cryptography.